U.S. DEPARTMENT OF ENERGY

NEVADA OPERATIONS OFFICE

NOTICE

NV N 205.X

Approved: 01-25-01
Expires: 01-25-02

NETWORK REMOTE ACCESS

INITIATED BY:
Safeguards & Security Division

1. OBJECTIVE. The timely exchange of information via data network connections is necessary for the routine functioning of the Department of Energy (DOE) Nevada Operations Office (DOE/NV), including its contractors. Accordingly, it is DOE/NV policy that access to information on automated information systems (AIS) should be maximized to the extent such access is reasonable and prudent, within the constraints of preserving and protecting the availability, confidentiality, and integrity (ACI) of sensitive and nonsensitive information alike. At the same time, remote access to cyber resources in any enclave, zone, or layered security level under the purview of DOE/NV is provided for the convenience of users. There is no inherent right to remote access and remote access privileges may be revoked for cause.

2. CANCELLATION. None.

3. APPLICABILITY.

   a. DOE/NV Elements. The provisions of this Notice apply to all DOE/NV organizational elements.

   b. Contractors. Requirements applicable to DOE/NV Performance-Based Management Contractor, security services contractor, national laboratories, other federal agencies, and other organizations (users) of DOE/NV computer resources are set forth in the Contractor Requirements Document, Attachment 1.

4. REQUIREMENTS. All organizations and users shall comply with the technical and administrative requirements contained in the attached Remote Access Requirements Document, Attachment 2, within 120 days from the date this Notice becomes effective. This Notice is not applicable to classified remote access (RED networks).

5. RESPONSIBILITIES.

   a. Director, Safeguards & Security Division (SSD). Approves Cyber Security Plans required by the attached Remote Access Requirements Document, Attachment 2. These plans will be included in the Cyber Security Program Plans as attachments.

b. Information Security Operations Manager (ISOM).

(1) Reviews and ensures the adequacy of plans prepared in response to this Notice.

(2) Recommends to the Director, SSD, approval of remote access plans that are in compliance with the requirements of this Notice.

(3) Conducts periodic audits and/or inspections of remote access users authorized under this Notice.

(4) Provides planning and documentation guidance to organizations with a need for remote access to DOE/NV community cyber resources.

c. Information Security Site Manager.

(1) Reviews and ensures the adequacy of plans prepared in response to this Notice.

(2) Recommends to the ISOM approval of submitted plans for remote access that are in compliance with the requirements of this Notice.

(3) Ensures that protective measures for remote access are in operation prior to the implementation of an approved plan.

(4) Conducts periodic audits and/or inspections of remote access users authorized under this Notice.

(5) Certifies that adequate safeguards are in place to prevent misuse of government-furnished remote access connections.

(6) Maintains documentation on all approved remote access justifications.

(7) Provides planning and documentation guidance to organizations with a need for remote access to DOE/NV community cyber resources.

(8) Ensures that all remote users of DOE/NV community cyber resources sign an acknowledgment of their responsibilities in the protection of DOE/NV sensitive and nonsensitive information in a remote environment.

(9) Immediately reports to the ISOM any incidents or occurrences that compromise, or have the potential to compromise, government information or access to government resources, or any activity that is in violation of this Notice.

(10) Ensures the preparation and execution of a certification test plan for proposed remote access services. Submits successful results of the test to the ISOM with the recommendation for approval of the service.

(11) Conducts a comprehensive review of remote access accounts and resources at least annually to ensure that account and service information is correct and continued use is needed.

(12) Ensures that the organization sponsoring remote access delegates a "Responsible Manager" to perform the defined functions associated to that role as specified herein.

d. Responsible Network Remote Access Program Manager in Organization Sponsoring Remote Access.

(1) Ensures that plans executing defined cyber security policies and standards are implemented.

(2) Develops criteria for authorizing remote user access.

(3) Approves user requests for remote access.

(4) Certifies that remote access is necessary for remote user.

(5) Establishes and maintains remote access accounts for remote users.

(6) Ensures that government-furnished remote access services/accounts are terminated when the requirement ends.

e. Remote Access User.

(1) Ensures that required protections are implemented to protect the ACI of DOE/NV resources and information are implemented and maintained. At a minimum the following are required:

(a) Password protects screens that provide remote access to DOE/NV resources and information.

(b) Constrains the location and operation of computing equipment with remote access to DOE/NV resources and information to an environment that does not present vulnerability for unauthorized access and use.

(c) Protects remote access information, including executable files or information (user IDs, passwords, dial-up access numbers, hardware/software keys, network configuration information) from unauthorized disclosure or access.

(2) Limits remote access use to the amount of time necessary to perform necessary tasks.

(3) Adheres to all DOE policies and procedures established for appropriate operation and use of DOE/NV computing resources.

6. REFERENCES.

a. DOE M 200.1-1, TELECOMMUNICATIONS SECURITY MANUAL, dated 3-1-97.

b. DOE N 205.1, UNCLASSIFIED CYBER SECURITY POLICY, dated 7-26-99.

c. Use of Warning Banners on Departmental Computer Systems, Memorandum, dated 6-17-99.

d. Guidance for Preparation of Acceptable Use Agreements for Users of Computational Resources, dated December 1995, revised June 1998.

7. DEFINITIONS.

a. Remote Access. Remote access is any connection from outside the DOE/NV enterprise into the enterprise. This includes modem/dial-in access to the private segment of the Information Protection Network (IPN) and Virtual Private Networks, or other remote connections, to the public segment of the IPN.

b. Zone. A network or subnetwork within which there is no effective isolation, e.g., firewall, between individual users, AIS, subnetworks, or networks. Data stored within the zone have a common access sensitivity or need to know.

c. Layered Security. Cyber security architecture consists of different isolated zones that require different security precautions. DOE/NV has identified three different security layers, they consist of RED for classified networks, YELLOW for networks that contain unclassified sensitive information, and GREEN for networks that consist of nonsensitive unclassified information. Zones that have one sensitivity level (RED, YELLOW, GREEN) will be isolated and protected from different security layers.

8. CONTACT. Questions concerning this Notice should be addressed to SSD at (702) 295-2212.

Kathleen A. Carlson
Manager

CONTRACTOR REQUIREMENTS DOCUMENT

Department of Energy (DOE) Nevada Operations Office (DOE/NV) contractor, Nevada Test Site user agencies, and National Laboratories shall:

1. Establish and implement procedures that conform to all network remote access policies and requirements as defined within the DOE Remote Network Access Notice.

2. Identify and assign personnel, as necessary, to perform the functions defined as Information Security Site Manager by this Notice.

3. Establish and implement all necessary reporting to the DOE/NV Information and Information Security Operations Manager (ISOM).

4. Implement the necessary “Remote Access User” training/orientation, within their organization, to ensure compliance with this Notice.

5. Ensure that technical staff implementing these policies are current on all technologies deployed in support of this Notice.

6. Make provision to extend these requirements as necessary to their subcontractors.

7. Provide ISOM immediate notification of any overt violations or noncompliance to this Notice.

REMOTE ACCESS REQUIREMENTS DOCUMENT

Minimum Requirements for Remote Access to the Department of Energy (DOE) Nevada Operations Office (DOE/NV) Cyber Assets.

1. Remote users are responsible for the protection of information at their remote locations. The protection provided to government information at remote locations shall be equivalent to the protection provided within DOE/NV facilities. Protection shall include the access method (e.g., user ID/password) and identifiers used for remote access and any information intentionally or inadvertently (e.g., temporary or history files) downloaded to the local system.

2. Any remote connection, once established, must be protected from unauthorized access whenever the remote system is unattended. This access control may be provided by physical security (locked office) or technical security (password protected screen saver set for less than 15 minutes) methods.

3. Where local user communities exist that have remote access or information protection requirements that differ in a security-significant manner (i.e., nonsensitive information only, Unclassified Controlled Nuclear Information, Privacy Act information), separate local user zones may be defined, established and maintained for each user community. Each zone shall have a clearly specified responsible authority (owner) and common membership characteristics. The responsible authority for the zone or security layer shall be required to identify the risks inherent in the level of security provided to the security zone. The responsible authority for a zone shall be required to provide assurances to authorities of other zones that their risks are not increased by the security posture of the zone or remote access permitted into the surrounding zone(s). Risks from entities outside of the DOE/NV enterprise (non-DOE/NV entities) will document the appropriate security precautions/procedures with a Memorandum of Understanding (MOU). The MOU should be attached to the Remote Access Security Plan.

4. The level of protection and rules for granting or denying access to all automated information systems (AIS) within a specified zone shall be equivalent.

5. An organization proposing remote entry into a zone of AIS shall demonstrate that the integrity of the zone is preserved when remote access is granted. A Remote Access Security Plan shall be prepared for this purpose, submitted through the Cyber Security Managers (Information Security Operations Manager, Information

Security Site Manager) for approval prior to implementation. The plan should also include a certification test plan. The scope of the security plan shall be comparable to that defined in OMB Circular A-130 for general support systems, including details regarding relevant security controls, authorizing, creating and disabling user accounts, and the degree of access (e-mail versus full network access) provided to each user. These plans will be incorporated into the organizational Cyber Security Program Plans (CSPP) and also be approved in accordance with the CSPP change management procedures. Authorizations for remote access are valid for a 1-year period. Continuing remote access and remote access methods in use for extended periods of time require review and recertification annually.

6. Perimeter-based security shall be implemented on all entry points into a defined zone or level of AIS, to include robust, auditable user identification and authentication. All entry points into a zone of computers shall be monitored for indications of attempts at unauthorized access.

7. Host-based security shall be implemented on all AIS within a zone to the degree appropriate to ensure the ACI of the information processed or stored on the AIS. Security provided shall be commensurate with the sensitivity and value of information in the cyber zone being protected and accessed, when evaluated against the potential user community.

8. Encryption shall be used for the protection of all passwords that allow access to computing resources behind the DOE/NV firewall, if the passwords pass across the Internet or other uncontrolled dedicated data circuits (does not include Pesticide Safety Team Network). All sensitive information transiting the Internet or other uncontrolled data circuits shall be encrypted. Encryption in this context shall meet the requirements of DOE M 200.1-1, TELECOMMUNICATIONS SECURITY MANUAL.

9. DOE/NV retains the right to inspect and audit all remote user locations and all computer systems employed under this Notice.

10. Foreign nationals may not be granted access to DOE/NV AIS under this Notice. Measures to preclude such access shall be included in the plans for any organizations that employ foreign nationals at locations where remote access is supported.

11. Personally owned or company/subcontractor-owned equipment and software may be used in conjunction with this Notice for connection to GREEN networks, at the

owner's risk. Remote access client software purchased by the government may be installed on personally owned or company/subcontractor-owned computers in support of validated need for remote access, provided the required waiver is signed and user authorization is obtained.

12. DOE/NV assumes no liability for accidents, loss, or damage on the part of contractors or contractor employees resulting from remote access incidents.

13. Wireless remote access is not authorized.

14. All Virtual Private Network (VPN) servers will be placed on the public segment of the Information Protection Network.

15. The following table summarizes some of the key security features for remote access:

Protection Measure	YELLOW	GREEN
Password protected screen saver	X	X
Encrypted data files or hard drive on the user side	X	
Use privately owned computer to connect to network		X
User authentication upon login	X	X
DOE banner presented upon login	X	X
Encrypted (VPN) connection	X	
Foreign national remote access	None	None
Wireless remote access	None	None